Future Proofing the EVSE:
Bridging Communications between Secure End Points (Grid and EV)

Proposal from VGI working group members Josh McDonald, George Bellino, Mike Bourton, Abigail Tinker, Lance Atkins, Rich Scholer, Dave McCready, Bill Boyce, Ralph Troute, Dean Taylor, Jim Tarchinski, Jordan Smith, Jeremy Whaling, Robert Ryueki

Oct 15, 2017

Background

September 2016

ACR ruled that IOU electric vehicle infrastructure procurement applications must require support for ISO 15118 as an EVSE to EV communications protocol or justify why they wouldn't require support

Spring 2017

After much discussion due to divergent stakeholder viewpoints, the CPUC along with four other CA agencies created the VGI Working Group to evaluate communications protocols and recommend if none, one, or many should be required for IOU's SB 350 TE behind-the-meter programs and investments

Present

The VGI Working Group is assessing VGI requirements, EVSE-to-EV protocols that could enable those requirements (**Deliverable 1**), and the costs/benefits of adopting each potential protocol (**Deliverable 2**)* to enable end-to-end (grid to EV and back) solutions

*http://cpuc.ca.gov/vgi/

Proposal: Evaluate an Additional Option in Deliverable 2 on its Merits

Future-Proof EV Infrastructure	**Evaluate an "EVSE Bridge" solution that allows communication technologies the flexibility to develop, mature and expand with the growing EV market**

1 All non-level 1 AC EVSEs* deployed in IOU BTM programs must be **capable of communicating VGI data back and forth between the EV and the grid (PFE/BMS) using an EVSE Bridge,**** without having to translate applications

2 Allow the voluntary use of **alternative communications paths** (e.g. telematics), that are currently available

Solution Also Allows for:

-Any "upper layer" application protocols for VGI communications

-Any physical media* (e.g. WiFi or cellular) to be used

*DC EVSEs may be the end point or may support the bridging function proposed here

**A communications module with EVSE bridge firmware that connects EV-EVSE communications to the external communication of choice (e.g., Wifi, Cellular, Zigbee, Ethernet) and passes the information between the two points without opening the information (e.g., like a post-office). The module does not contain any application protocol. See appendix for details on protocol layers description of upper layers and physical media.

Concerns Regarding Selecting a VGI Communication Application Protocol

- Sufficient empirical evidence does not exist today that supports the benefits of one VGI communication application protocol over another for EV adoption, customer ease of use, customer choice, market transformation, etc.
- EVs do not currently support any high-level communications for AC charging
- Actual costs for stakeholder deployment of any application cannot be provided and are thus subjective and debatable
- Well-known near-term grid applications and functionality (e.g., load management, cybersecurity, integration of distributed energy resources) must be supported by VGI communication applications. *HOWEVER* different applications and functionality will emerge and need to be deployed
- Any VGI communication application mandate will not align with all stakeholders interests
- Different market segments have different needs regarding VGI communications technologies and functionality
- Communications from the building management system (BMS) or power flow entity (PFE)* supports Internet Protocol (IP) based communications which allows for VGI communication applications to be routed from remote sources to a destination and bridged between different physical media (Internet, Cellular, Wi-Fi, Ethernet, etc.)

*A PFE is an off-site entity or entities that is requesting or mandating VGI activities from other actors downstream. The PFE is broad term than may include the Aggregator, Utility, Site Host, EV Service Provider, Energy Service Company, Alternative Energy Supplier, Energy Portal, or Clearing House

Benefits of Future-Proofing EV Infrastructure with EVSE Bridge

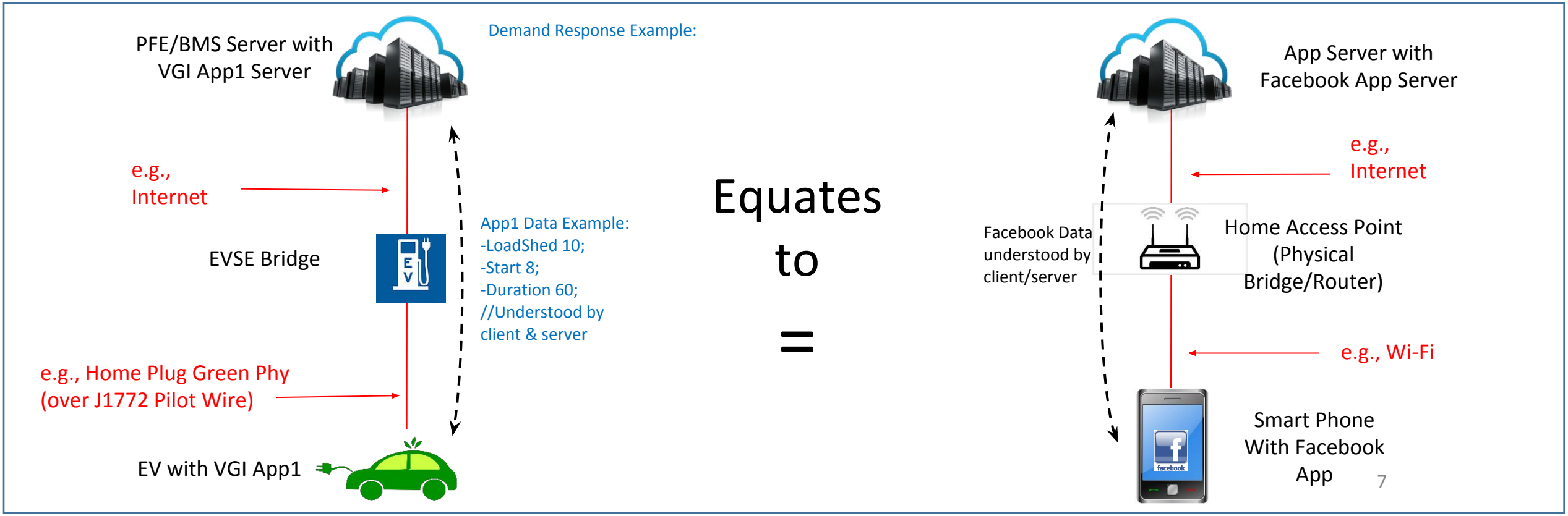
Enables Customer Choice	• Allows the use of any VGI internet-based application if supported by PFE/BMS and the EV • Allows for alternative communication paths if EVSE bridge is not available or preferred (e.g. telematics). • Reduces vendor lock-in by standardizing the EVSE with simple EVSE bridging technology and allows users to swap service providers easily
Provides Flexibility	• Allows for different VGI communication applications to be used for different deployment scenarios. • Does not predict what will be supported in the future (e.g., what occurred with ZigBee in smart meters) • Allows for upgrading of legacy EVSEs by adding interface cards supporting routing and selected physical layers • Enables other communication pathways to the EV beyond PLC
Low-Cost Solution	• Minimizes stranded asset risks by not requiring EVSE-centric VGI communication applications • Minimizes EVSE software deployment, support and upgrade costs • Removes cost and complexity of maintaining multiple VGI communication applications on the EVSE and their mapping to each other when either receives an update*
SECURE	• Minimizes cyber security vulnerabilities by bridging routing VGI communications between PFE/BMS and EV rather than de-encrypting and re-encrypting at the EVSE security • Does not require permission from an in-between point for VGI communications between grid and EV

*Because 2 different communication protocols are not needed to go end-to-end. Avoiding this mapping and update complexity eventually becomes. A significant burden when there are many different service providers that are required to update hundreds of thousands of EVSEs. See appendix for pictorial representation

BACK-UP

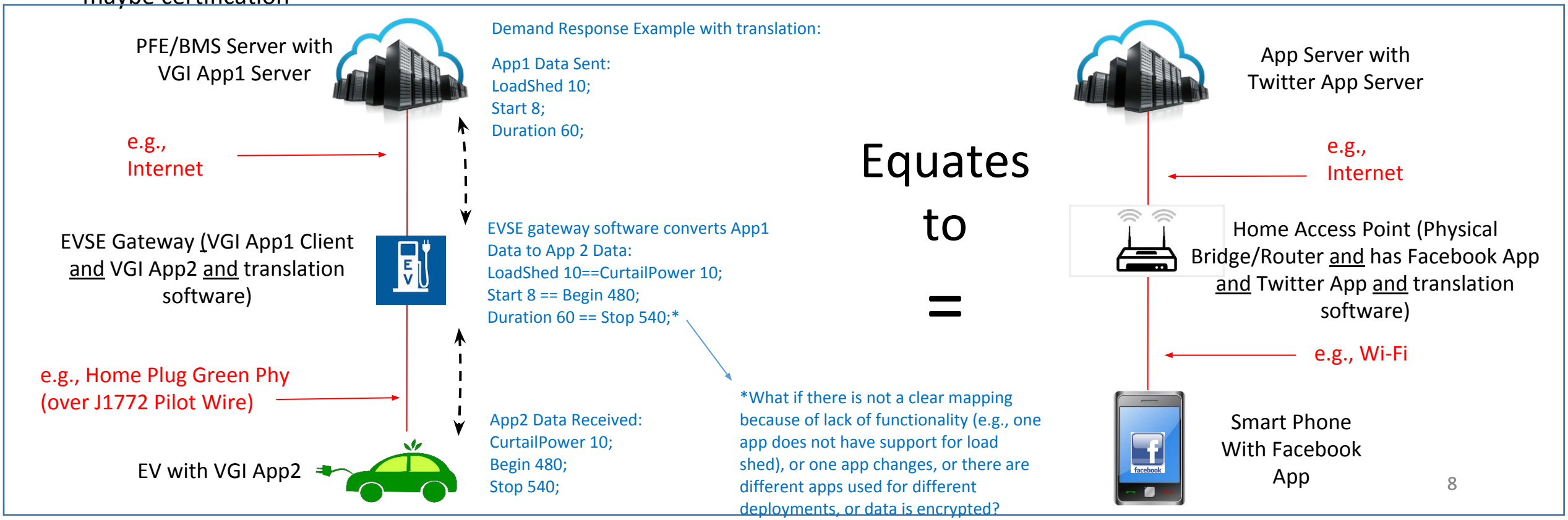
EVSE Bridging Communications Analogy- EVSE and Home Access Point/Router

- Server (e.g., PFE/BMS or App server) and end node (e.g., EV or Smart Phone) both support the application protocol (e.g., VGI App1 or Facebook in the picture)
- EVSE/Home Access Point only looks at lower 'Media' layer information (e.g., source & destination addresses) to pass on the application data but cannot look at the application data (AppX and Facebook data passed through EVSE/Home Access Point)
- Could add other apps to EV/Smart Phone if other functionalities are desired (e.g., Twitter, VGI App2, etc.)
- Could remove EVSE as sole communication path

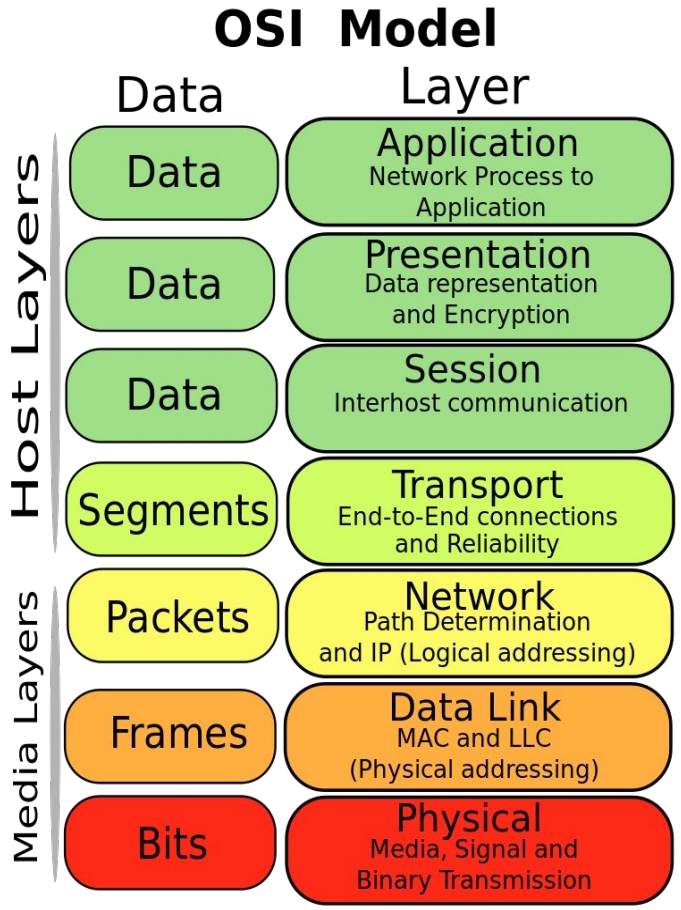


When two different application protocols are used

- EVSE/Home Access Point still bridges/routes data but must support both applications plus a translation software (aka Application Gateway)
- How date is translated must be agreed to by Server and Client and be implemented the same way across all EVSE/Home Access Point vendors. This should require Standards Development Organization's development and maintenance, Testing, Certification (Who? Time?)
- Both apps and translation software must be maintained by all EVSE/Home Access Point Vendors, especially when either application is updated breaking the existing translation. Requires above Standards Development Organization mapping update, Testing and maybe certification

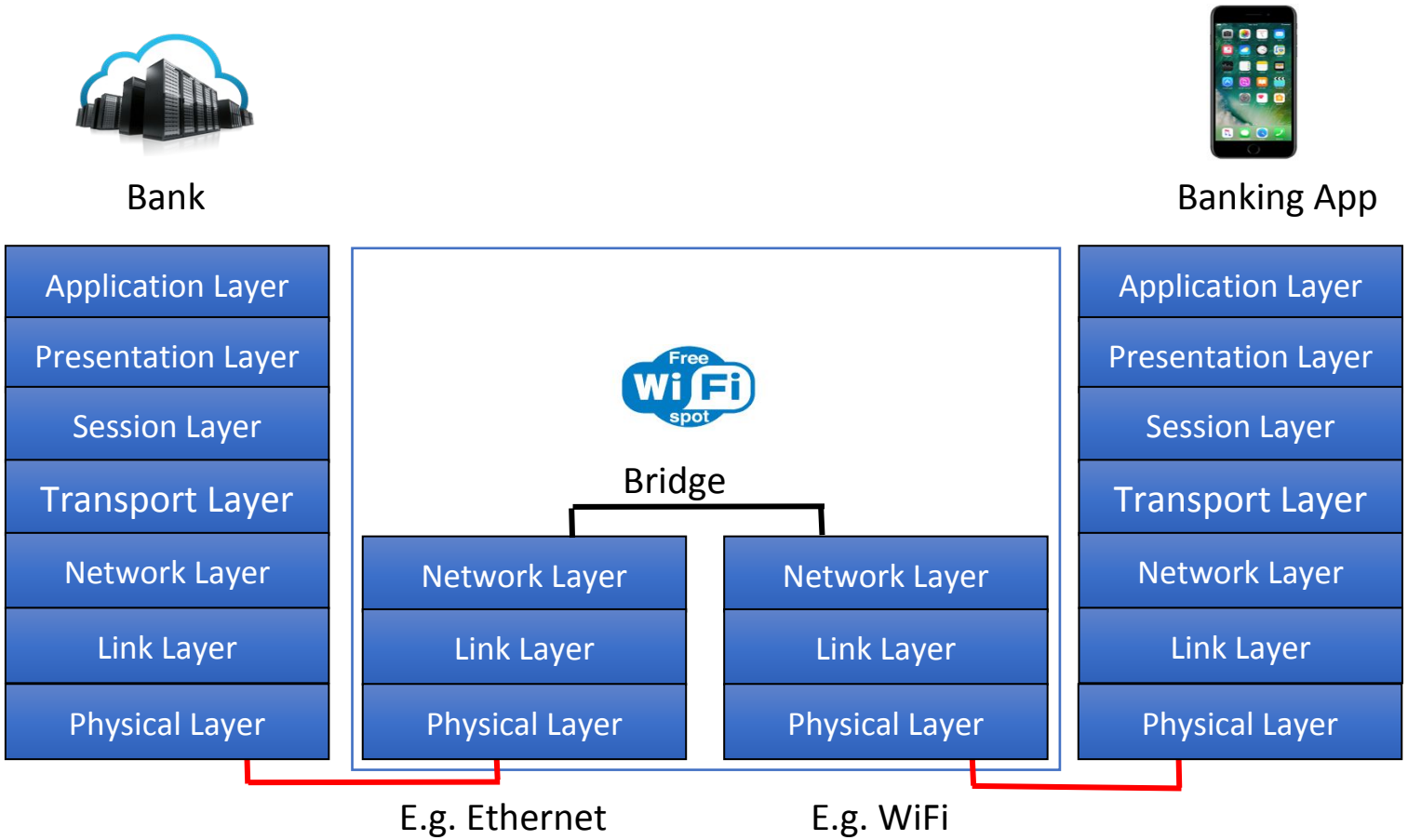


Primer on the OSI model



- Open Systems Interconnection (OSI) Model describes communications between two computing systems by separating functionality into 7 layers.
- Upper ‘Host’ layers deal with application data, authentication, authorization, connection, encryption/decryption
- Lower ‘Media’ layers deal with moving upper layer data between networks and from source to destination
- Networks operate on one basic principle: "pass it on"
  - Each layer takes care of a very specific job, and then passes the data onto the next layer

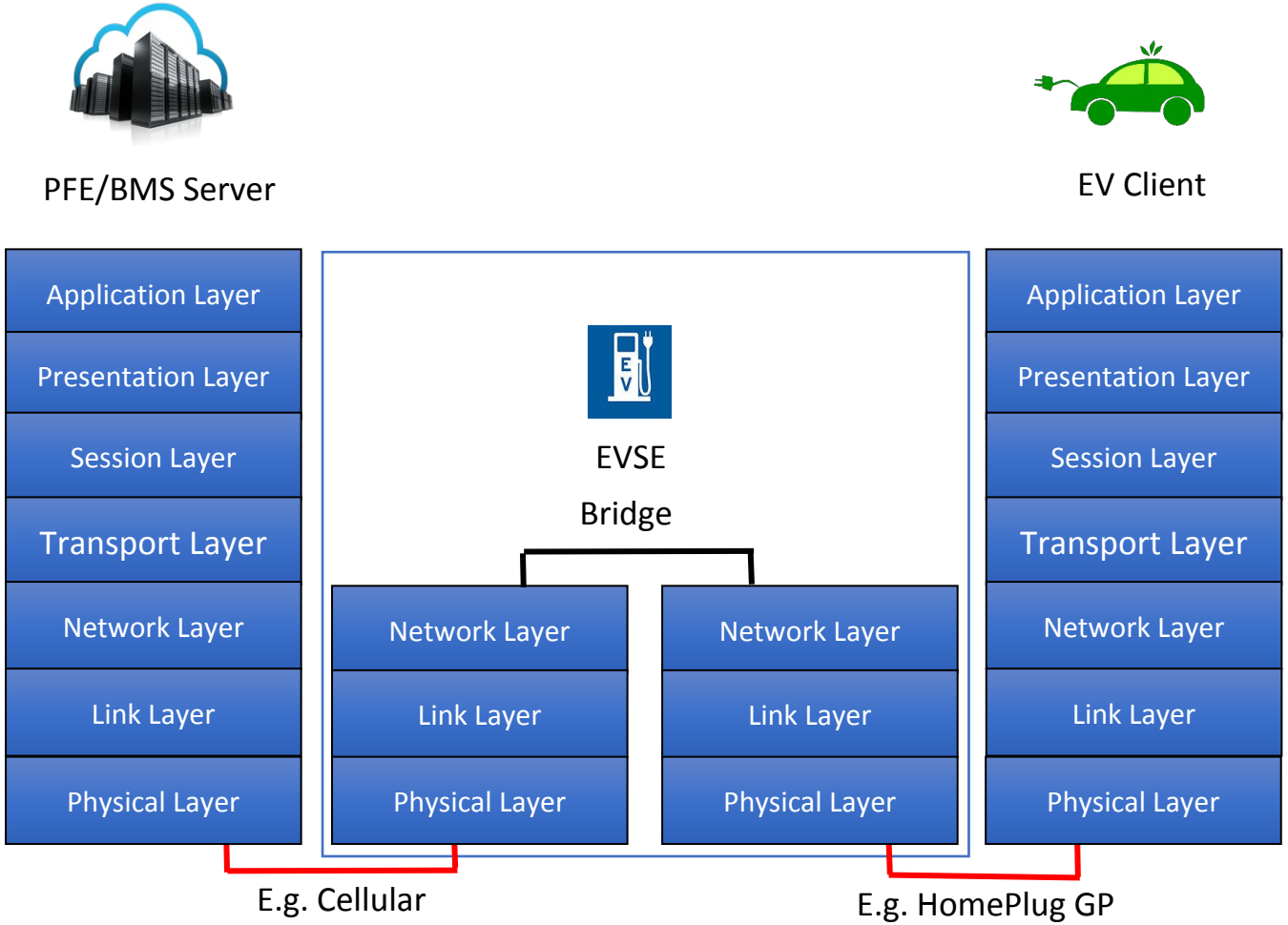
Analogy: How the Internet secures your apps so your transactions are safe



The information is carried in the Application Layer and is encrypted and the encyption keys are only known by the Server and Client
Any device (E.g. Public WiFi Hotspot) between the Server and the Client uses the lower layers only to bridge, switch or route the packets

Definitions:
Bridge is connecting two different physical layers
Switch is to connect two same physical layers
Route is to connect two different networks e.g. Home and the Internet

Similarly, EV Communications are Now Cyber Secure as the EVSE Bridges VGI Communications at the Network Layer and Cannot Decrypt the End-to-End Communications



EVSE Complies with [NISTIR 7628 Guidelines for Smart Grid Cyber Security]

Future Proofing the EVSE Reduces Complexity and Cost

- The use of a single end to end application protocol that uses an EVSE bridge allows for:
  - Less entities/costs required for updating application when revisions occur
  - A single certification process
  - A clear understanding (semantics) of what requests/data are intended to convey as the same application functionality/syntax is supported
  - Allows for simple firmware updates to bridge/router (can be done by user or locally)
- The use of two VGI communication application protocols to go end-to-end:
  - Requires a third entity/costs that must maintain and update both VGI communication (VGIC) applications when revisions occur
  - Requires a gateway to translate between VGIC applications
    - Must have agreement (mapping) of what one VGIC applications request/data means for the other (semantics) and what parameters (syntax) is used
    - Must be updated whenever one of the VGIC applications is updated
    - Functionality is not limited by one or the other VGIC application
    - Must be standardized/certified globally as opposed to per implementation

Cybersecurity Benefits Of the Future Proofing Proposal

- End to End VGI communications allows application data to be encrypted between source and destination (e.g., PFE to EV) ensuring privacy and confidentiality
  - Only source and destination hold keys and able to unencrypt, utilize data
  - Personally Identifiable Information (PII) or data that can be used to calculate PII only held at source and destination, encrypted in transit
- Authentication (you are who you say you are) and Authorization (you have permission to charge) occurs at the building management system or power flow entity
  - The EVSE does not say you are allowed to charge
  - In the analogy in the chart above, the Home Access Point does not say you are allowed to use Facebook
- When 2 separate VGI communication applications are used in series to go end-to-end, intermediary (e.g., EVSE/Home Access Point) must unencrypt data in order to map it to the other application via translation software
  - Separate keys maintained in EVSE/Home Access Point
  - Susceptible to man in the middle attacks- Interloper pretends to be source or destination
    - Can modify controls or other requests which may impact drivers, site hosts or grid or intercept PII or send malicious code